マルチエージェント環境におけるプライバシアウェアな最適化・学習

著者	佐久間 淳
発行年	2010
その他のタイトル	Privacy-aware Optimization and Learning in Multi-agent environments
URL	http://hdl.handle.net/2241/107738

様式 C-19

科学研究費補助金研究成果報告書

平成 22 年　4 月　19 日現在

研究種目：若手研究(B)
研究期間：2008～2009
課題番号：２０７００１３０
研究課題名（和文）マルチエージェント環境におけるプライバシアウェアな最適化・学習

研究課題名（英文） Privacy-aware Optimization and Learning in Multi-agent environments

研究代表者
佐久間 淳（SAKUMA JUN）
筑波大学・大学院システム情報工学研究科・准教授
研究者番号：90376963

研究成果の概要（和文）：この研究プロジェクトでは分散秘密情報源からの学習と最適化問題に関するアルゴリズム構築、セキュリティの検証、性能評価などを行った。対象アルゴリズムとして、巡回セールスマン問題、強化学習、および、分類器学習における前処理・後処理を扱った。これらのアルゴリズムを分散環境でセキュアに実行するために、準同形性公開鍵暗号等を利用したプロトコル設計を行った。また提案アルゴリズムのセキュリティを保証するための証明および計算効率性を検証するための計算機実験を行った。

研究成果の概要（英文）：In this research project, learning and optimization from privately distributed data sources have been studied. Specifically, algorithm design, security, and performance evaluation has been considered. The traveling salesman problem, reinforcement learning, and pre/post-processing of classification tasks have been focused as target algorithms. In order to securely perform these algorithms with taking privately distributed information, protocol are specifically designed for each algorithm by making use of homomorphic public-key cryptosystem. Furthermore, we proved the security of these protocols. The assessment of the computational efficiency has been performed experimentally.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	2,100,000	630,000	2,730,000
2009 年度	1,300,000	390,000	1,690,000
年度			
年度			
年度			
総　計	3,400,000	1,020,000	4,420,000

研究分野：機械学習、知識発見、セキュリティとプライバシ
科研費の分科・細目：情報学・知能情報学
キーワード：プライバシ

１．研究開始当初の背景

多様なシステムの統合を通じたシステムの全体最適化や、複数の個人や自律エージェントの行動履歴に基づいたレスポンスの適応学習など、分散した情報源から構成される最適化や学習と、それに基づく高度なサービス

の実現への社会的ニーズが高まっている。
一方、個人情報保護法の施行や日本版ＳＯＸ法の法制化に伴い、機密情報や個人情報の取り扱いには厳密な管理が強く求められている。プライバシを保護した計算技術としてプライバシ保護データマイニング(PPDM)が注目を浴びつつあったが、実社会の多くの問題はマルチエージェント環境下での最適化問題として解釈できる場合が多い。

２．研究の目的

研究代表者は、PPDM に着想を得た発展として、プライバシ保護型計算の最適化への適用可能性を検証することを目的とし、以下の課題を設定した。

(1) 組み合わせ最適化問題における PPO の汎用的なモデル化とその最適化、

(2) マルコフ決定過程における PPO のモデル化とその最適政策の強化学習、

(3) 分類学習問題におけるプライバシ保護型前処理・後処理

(1)が対処しようとしている問題は、以下の問題意識に基づく。組み合わせ最適化問題におけるプライバシ保護をカーナビの経路探索サービスを例に説明する。経路探索サービス提供者 A は、任意の二地点間の移動時間をリアルタイムに予測しているが、地点間移動時間の計算法は企業秘密であり公表したくない。またユーザーB は複数の地点を経由して移動しようとしており、最も移動時間が少ない経路を求めたいが、訪問地点群は個人情報であるためやはり公表したくない。果たして、A と B は互いの秘密情報を明かすことなく最適経路を探索することができるだろうか？

ここで例にあげた経路探索問題は、移動コストおよび移動地点という二つの個人情報あるいは機密情報に依拠した最適化問題である。遺伝的アルゴリズムをはじめとするメタヒューリスティクスは、最適化対象であるコスト関数をブラックボックスとしたままで最適化が実行可能であるという意味において、プライバシ保護を必要とする最適化問題のためのソルバーに適している。この研究では、プライバシ保護を考慮した組合せ最適化問題を、暗号学的ツールと遺伝的アルゴリズムを利用して解決する方法を提案する。

(2)が対処しようとしている問題は、以下の問題意識に基づく。ネットワーク環境の発展に伴い、物理的エージェントやソフトウェアエージェントによって収集される多様な情報を横断的に収集することが可能になりつつある。分散強化学習は、このような分散化された情報源に基づき、複数のエージェントが長期的な利得を最大化するための確率的な制御側を、環境に対する知識なしで獲得することを目指す枠組みである。従来の分散強化学習は、通信帯域の制約など、物理的な制約のために、分散化された観測の完全な統合が困難であることを想定しており、その制約下における準最適な制御側の効率的な学習が追求されてきた。一方、この研究では、機密保護やプライバシ保護などの社会的制約のために、分散化された情報源からの観測の統合が困難である状況を想定する。このような制約に対処するために、この研究では公開鍵暗号や Secure Multi-party Computation と強化学習を組み合わせる。提案アルゴリズムでは、複数エージェント間の観測を一切共有することなく、最適な制御則のみを学習する方法を研究する。

(3)が対処しようとしている問題は、以下の問題意識に基づく。プライバシ保護分類は、分散した秘密データの和集合を用いて学習させた分類器と同様のものを、互いにデータを共有することなく学習させる手法である。既存のプライバシ保護分類は、既存のデータマイニングアルゴリズムを、プライバシが保護されるように改良することに力点が置かれていた。しかしながら、データマイニングの全体のプロセスにおいて、その効用を高めるためには、データマイニングの実行部分のみならず、属性選択やモデル選択など事前/事後処理が重要である。この研究では、秘密分散データから、その予測結果を共有することなく様々な分類器においてモデル選択や属性選択を実現することを目指す。

なお、(1)、(2)は申請書記載の課題、(3)は申請書の範囲を超えた発展的な課題である。

３．研究の方法

(1) 分散した秘密情報によって定義される組み合わせ最適化問題において、問題を定義するインスタンスを秘密情報とみなし、このような秘密の分割インスタンスによって定義される一般の組み合わせ最適化問題を、整数計画問題を経由し、局所探索や遺伝的アルゴリズムなどによって解くアルゴリズムを開発した。また構成されたプロトコルが、各エージェントの秘密情報を確かに漏えいしないことを定理として証明し、セキュリティを保証した。

(2) 分散した秘密情報源からの強化学習では、マルコフ決定過程における状態・報酬観測、行動出力の分割モデルを各エージェントのプライバシーとみなし、定義されたプライバシーおよび分割モデルに対応したマルコフ決定過程のためのプライバシアウェアな強化学習法を開発した。また構成されたプロトコルが、各エージェントの秘密情報を確かに漏えいしないことを定理として証明し、セキュリティを保証した。

(3) 分散した秘密情報によって定義される分類器学習における特徴選択・モデル選択に関する研究を行った。分類機学習の前処理・後処理としてはそれぞれ特徴選択とモデル選択が分類性能向上のための重要である。そこで、秘密情報源から作成された分類器より、データの秘密をあかさずに分類性能を評価することができる Hamming distance プロトコルを提案し、安全な分類性能評価法を確立した。またこれに基づき、実際にプライバシ保護データマイニングの前処理・後処理として、k-fold cross validation を通じたプライバシ保護特徴選択・モデル選択を単純ベイズ分類器やサポートベクターマシンに適用し、その有効性を検証した。

４．研究成果

(1) 提案法の効率性を実験的に評価した。プライバシ保護ローカルサーチ(PPLS)においては、比較あたりの変更枝数は一定のため、都市数にかかわらず比較あたりの計算時間は一定でとすることができた。一方、プライバシ保護遺伝的アルゴリズム(PPGA)では変更枝数は都市数に応じて変化し、実験では比較あたりの時間は都市数に対して概ねおおむね線形に増加するアルゴリズムとなった。実験結果からは、10%の誤差率が容認できるならば数時間で計算を終了する PPLS が合理的な選択であるとの結論を得た。 PPGA の利用は極めて高精度な解の発見が期待できるが、収束には数日程度を要するため、大規模計算を行うためには並列が必須であるといえる。それでもなお、高精度な最適化が必要な場合は、PPGA の計算速度は PPLS よりも少ないことから、このような場合には、PPGA の利用が合理的であると言える。プライバシ保護型 GA/LS の計算時間は大規模問題においては十分小さいとはいえないが、実験において、計算は現実的な時間で完了することが検証ができた。計算の高速化や他問題への拡張等が将来の課題である.この研究は、2007 年に遺伝的アルゴリズムにおいて最も大規模な国際会議である GECCO で発表したアルゴリズムの一般化であり、2008 年 12 月に進化計算研究会で発表した。またこの研究について、IEEE CISJ Young Researcher Award を受賞した。

(2) 強化学習におけるプライバシモデルとして、経験系列を時間で分割するモデル(partitioned-by-time)と観測・行動の属性で分割するモデル(partitioned-by-observation)の定義を与えた。このプライバシモデル上で、学習手法として Q 学習および SARSA 学習を安全に実現するプロトコル、および、ε-greedy 選択を安全に実現するプロトコルを与えた。負荷分散問題をシミュレートする計算機実験により、一更新あたり数分程度の計算時間で実行でき、かつ、プライバシを考慮しない場合と同様の期待報酬を獲得できることが検証された。この分散秘密情報源からの強化学習に関する研究は米国 Rutgers 大学との共同研究として行われ、機械学習にて最も権威ある国際会議である ICML2008 に採録され、2008 年 7 月にヘルシンキにて発表された。

(3) 分類問題における秘密情報は、「分類器」そのものが秘密情報を含む場合と、分類器による「分類結果」が秘密情報を含む場合に分けられる。この研究では、分類器自体が含む秘密情報の保護は考慮しない”regular classifier”と、分類器自体が含む秘密情報を保護することができる分類器表現である”privately shared classifier”の二種類の定義を与えた。また分類結果自体が含む秘密情報の保護は考慮しない”regular prediction”と、分類結果自体が含む秘密情報を保護することができる分類結果の表現である”privately shared prediction”の二種類の定義を与えた。これらの任意の組み合わせにおいて、安全にモデル選択や属性選択を実現することができる一般化 Hamming 距離プロトコルを提案した。プロトコルは、単純ベイズ分類器における属性選択およびサポートベクターマシンにおけるモデル選択において実装され、(1)モデル選択や属性選択自身が分類器や分類結果の秘密を漏らさないこと、(2)モデル選択や属性選択はプライバシ保護を考慮しない場合と同様に実現可能であること、が示された。この研究は、米国 Rutgers 大学との共同研究として行われ、国際会議である ACML2009 に採録され、2009 年 11 月に南京にて発表された。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 7 件）

1. Jun Sakuma and Shigenobu Kobayashi、Large-scale k-means clustering with user-centric privacy-preservation、Knowledge and Information Systems,（査読有, online）2009.

〔学会発表〕（計 7 件）

1. Jun Sakuma, Rebecca N. Wright: Privacy-Preserving Evaluation of Generalization Error and Its Application to Model and Attribute Selection。 ACML 2009: pp. 338-353, Nov. 3, 2009, Nanjing, CHINA.
2. Jun Sakuma, Shigenobu Kobayashi: Link analysis for private weighted graphs. SIGIR 2009: pp. 235-242, Jul. 21, Boston, USA.
3. Jun Sakuma, Shigenobu Kobayashi, Rebecca N. Wright: Privacy-preserving reinforcement learning, ICML 2008: pp. 864-871, Jul. 7, Helshinki, FINLAND.

〔その他〕
ホームページ等
www.slab.cs.tsukuba.ac.jp/

６．研究組織
(1)研究代表者
佐久間 淳（ SAKUMA JUN ）
筑波大学・大学院システム情報工学研究科・准教授
研究者番号：90376963